

Overview of Data Security Issues in Hospital Information Systems

Maslin Masrom

Razak School of Engineering and Advanced Technology
Universiti Teknologi Malaysia
maslin.kl@utm.my

Ailar Rahimly

Razak School of Engineering and Advanced Technology
Universiti Teknologi Malaysia
a.rahimly@gmail.com

Abstract

Nowadays, hospital information systems (HIS) provide real-time data and information in order to guide public health organizations especially in decision-making. The hospital information systems are integrated information systems designed to manage the administrative, financial and clinical tasks or aspects of a hospital. It plays an important role in planning, initiating, organizing and controlling the operations of the hospital, and a crucial role in providing quality healthcare services. The aims of this paper are to explore and provide a better understanding of data security aspects in hospital information systems, and add more body of knowledge in information systems (IS) field in the healthcare industry. The views of previous researches are presented and discussed, and new area of interest to the IS and HIS community then are proposed.

Keywords: Hospital information systems (HIS), Functions, Components, Data security issue, Information systems (IS)

Introduction

Hospital faces with several challenges and issues that related to store, share and distribute the patients' health records and hospital use manual methods that include pen, paper and human memory. The manually methods are not suitable and hospital need technological environment for reducing the medical error, improve the quality of services, cost effectiveness, timely decision-making, and growing the efficiency. To overcome these issues and challenges, the implementation of several innovation projects for providing the efficient healthcare services are introducing to the management of hospitals.

Currently, technology is playing important role in the several sectors. One of the sectors that need to use technology is a healthcare sector, to improve the quality of services. HIS are integrated information systems designed to manage the administrative, financial and clinical aspects of a hospital. The aim of the HIS is to achieve the best possible support of patient care and administration by electronic data processing. They provide the required information to each level of the management at the right time, in the right form, and in the right place, therefore the decisions could be made effectively and efficiently (Ismail et al., 2012).

The HIS have implemented in various hospitals for example Malaysia, Japan, South Korea and Australia. The purpose of HIS is to improve the quality and management of clinical care and hospital healthcare management in the areas of clinical process, analysis and activity-based costing. The main benefits of implementing HIS are improve the patient care and reduce the cost. HIS can improve quality of patient care by increasing the timeliness and accuracy of records and administrative information. The standardization of HIS improves cost control by improving efficiency and productivity, and HIS also provides increased security of patient information that can be accessed only by

those who need the information, for example, pathology, radiology and administrative offices. Nowadays HIS are in demand to assist the doctors, nurses, support staff, and hospital service with timely service and precision (Balaraman and Kosalram, 2013).

HIS expected to make the right information to the right people, in the right place, at the right time and in the right form whereby they improve patient care by assessing data and making recommendations for appropriateness of care. In this context, ensuring data security stored in the system is very important since the data that stored in this system related to the patient health record and this type of the data is so sensitive and valuable.

The main purpose to use HIS is to eliminate manual processing that it's major obstacle to increasing the performance of organizations in terms of efficient and fast health service (Kim et al., 2002). However, HIS implementation faces with several challenges and issues (Chang et al., 2007). HIS to provide efficient and fast services need to collect, process, transfer, store and access to patient information, this type of the information that related to patients are so valuable and sensitive, therefore, in turn lead to critical security issues (Liu et al., 2005). Hence, one of the areas that need to consider in the HIS is a security of patient data and information.

This paper investigates the using of the technology innovation in the healthcare sector and more consider in the HIS and describe the security issues that existing in the current HIS. This study contributes to the body of knowledge about HIS and data security issue in HIS, and it contributes to draw the attention of researchers and interested to do many studies and research in data security issue in the HIS. The result of this study could assist hospital to use technology innovation in the hospital system. Using the technology innovation in the hospital system lead to the improvement of the quality of the patients' services and also

help the system developer to know more information about data security issues in HIS and try to find solution for them. This study can make novel contribution in the context of healthcare sector to enhance and develop the more diffusion of IS in the hospitals that provide more benefits for patients and hospitals.

This paper has divided into four main sections, the following section describes the definition of HIS; second section presents the methodology; third section discusses about data security issues, and last section conclusions and future works the paper.

Definition of Hospital Information Systems

Many countries use IS for their healthcare sector to provide high quality service for their citizen. Electronic health (e-health), HIS, telemedicine, and electronic health record (EHR) are types of the initiative that generated by using IS to bring better healthcare services for patients and overcome challenges and issues such as storage cost, low quality services, share patients' records. Use of the IS in the healthcare sector is very slower than other sectors such as financial and telecommunication. Because of healthcare sector is very far to adopt IS in compare to the other sectors, while with adopting IS in the healthcare sector, this sector can provide high quality service for patients (Sulaiman, 2011; Jha et al., 2008).

HIS are a computer system that designs to manage the information of patient to improve the services and lead to the high quality healthcare treatment. Hospitals are considered as complex institutions with large departments and units coordinate care for patients, therefore they need efficient system to perform their job more efficiency

and effectively (Adler-Milstein and Bates, 2010). Today, hospitals are becoming more dependent on the capability of HIS to assist in the management, administration, diagnosis and education for improving services and practices. The HIS are one classification of health information systems with a hospital as healthcare environment. It consists of integrated hospital information processing systems. For examples: Computerized physician order entries that are also referred to as computerized provider order entry, patient care information systems, nursing (bedside) documentation systems, nursing IS, and general practitioner IS (Yusof et al., 2008).

According to Garrido et al. (2004) HIS consist of several applications that are integrated in order to capture data in specific sections of the hospital, handle the workflow of daily medical services, and also assist in managing financial, administrative and clinical data. Meanwhile, Biomedical Informatics Ltd. (2006) reported that HIS comprises two or more components such as Clinical IS, Financial IS, Laboratory IS, Nursing IS, Pharmacy IS, Picture Archiving Communication systems (PACS), and Radiology IS.

The goal of HIS is to use computer, communication equipment and internet to collect, store, process, retrieve and communicate patient care and administration information for all hospital activities. The system characteristics for HIS among others are: (i) Support healthcare activities at the operational, tactical and strategic levels; (ii) Encompass patient management, administration, facilities management and medical applications; and (iii) Contain database systems, data communication facilities and terminal or workstations. Figure 1 illustrates HIS integration model.

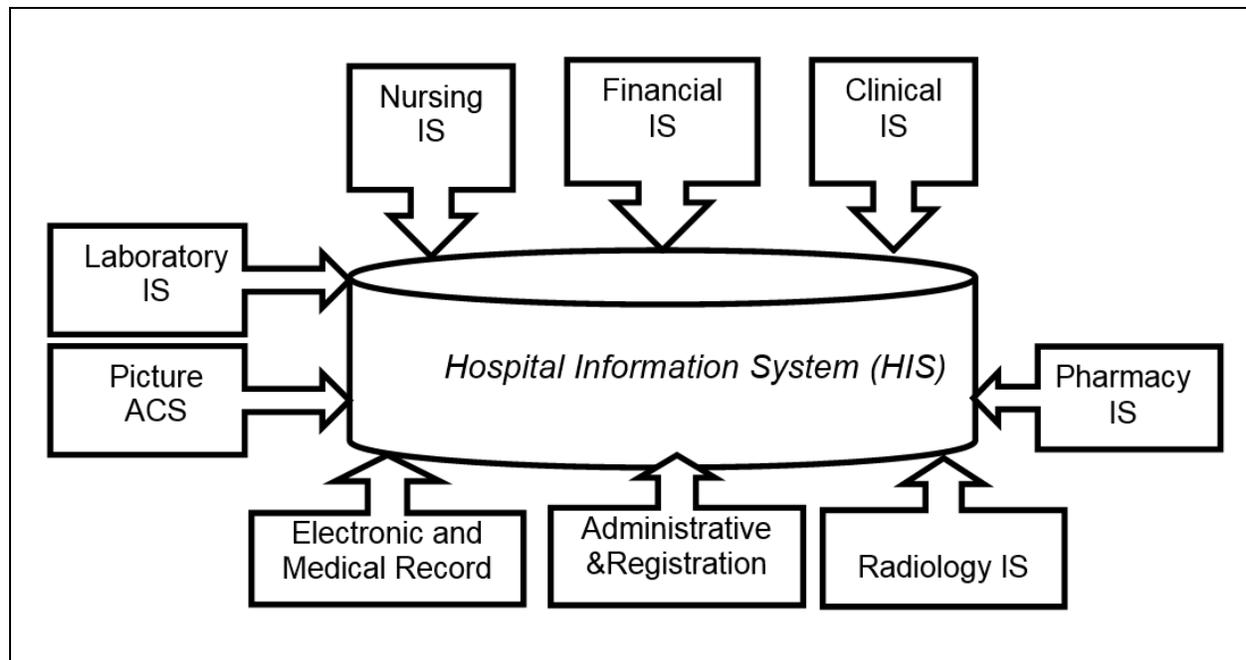


Figure 1 - Hospital Information Systems Integration Model

Note: Source: Biomedical Informatics Ltd. (2006).

Following are the brief description of the components of HIS integration model as shown in Figure 1.

- *Clinical IS:* Computer systems designed for collecting, storing, manipulating, and making available clinical information important to the healthcare delivery process.
- *Electronic Medical Record:* Digital version of paper charts that contains patient medical history, and mostly used by providers for diagnosis and treatment. It is a fully integrated knowledge repository that caters to medical and clinical records of patients in the hospital. This component supports medical professionals of various departments of the hospital with information like treatment histories, diagnoses, medical examinations and test results.
- *Pharmacy IS:* Computer systems designed to meet the needs of a pharmacy department. Using such systems, pharmacists can supervise and have inputs on how medication used in a hospital.
- *Radiology IS:* A computer system that assists radiology services in storing, manipulation and retrieving of information.
- *Laboratory IS:* A computer information system that manages laboratory information for all the laboratory disciplines such as clinical chemistry, hematology and microbiology.
- *Picture ACS:* A medical imaging technology, which provides economical storage of and convenient access to the patient image from multiple machines.
- *Administration and Registration:* A computer system that provides functions such as general administration consists of patient registration, medical registration, billing and a general inventory module.

- *Financial IS*: Computer systems that manage the business aspect of a hospital. While healthcare organizations' primary priority is to save lives and not making profits, they do acquire running costs from day to day operations including purchases and staff payroll.
- *Nursing IS*: Computer systems that manage clinical data from a variety of healthcare environments, and made available in a timely and orderly fashion to assist nurses in improving patient care.

Healthcare sector needs HIS to provide high quality healthcare treatment. In the European countries, United States and Canada used different technology to develop IS for healthcare sector to improve healthcare services such as EHR, smart card technology, Telehealth, Personal Health Record (PHR) and others. Although, many new technologies implemented in these countries but also they still have issues and challenges (Ahmadi et al., 2015). Asia and Singapore reach to the good level of IS influence in clinical and administrative activities in the seven main hospitals (Pan and Pokharel, 2007), while in Malaysia, in some HIS cover all aspect of hospital operation such as administrative, financial and clinical systems and need more system development (Sulaiman, 2011).

According to Ahmadi et al. (2015) it is about 85% of public hospital in Malaysia have delayed in adopting and implementing the HIS, and almost 15% of public hospital in Malaysia equipped with full integrated or partly integrated HIS. This statistic shows the trend of healthcare information systems progress among the Malaysia hospitals is very slow. While currently, the development in HIS is increasing to enhance the quality of patients' service and also reduce the cost and improve the access to the patient record (Ahmadi et al., 2015).

Many healthcare innovations (see Table 1) have implemented while some of them face with several challenges and issues (such as

security and privacy, high cost, and exchange data) and some of them overcome and not use in the healthcare sector. Electronic Medical Records (EMR) is one of the HIS innovative, which face with several challenges such as: security and privacy issues, implementation issues, ethical and legal issues and documentation reliability and the suitable solution for these issues are applying technological security and behavioral approach. EMR failed to implement in the Japan hospitals due to the high startup cost. Several barriers are available in the start phase decision to adopt the EMR system such as technical, behavioral, and economic (Kim et al., 2002; Paré and Elam, 1999; Ahmadi et al., 2015).

The main function of HIS is to provide collection, storage, processing, extraction of patient medical information, financial accounting, analysis, executive management information and decision analysis of statistical information and data communication, and fulfill information needs of all authorized users (Wei, 2011). Thus, hospital information systems can define as massive, integrated systems that support the comprehensive information requirements of hospitals, including patient, clinical, ancillary and financial management (Roussel et al., 2005; Yusof, et al., 2008).

According to Acharyulu (2012), HIS have evolved as an integration system of order entry systems, an administrative system, and departmental subsystems within a hospital. It has become necessary for every healthcare staff in a hospital to use a computer terminal at almost every day's work. In this context, HIS could provide various information for making decision and good communication environment for healthcare staff.

The existing HIS that use in the several hospitals facing with several problems. The main problem in HIS is data storage and transmission, lack of the same format of the data is major problem to communication the data among the several hospital system and also when the number of the patient

increase, HIS need to increase the storage that lead to increase the hospital cost. As a result, sharing the patient information among the several, HIS is impossible and hospital all the time needs to develop the storage. The second problem, related to high setup cost. The cost for implementing the HIS that integrates all types of the hardware and software is so expensive (Ratnam and Dominic, 2012).

At the same time, HIS have several benefits and issues for implementing. Using HIS for hospital brings many benefits that include save time and space, reduce the medical

error, more accessibility, more accurate, and improve the patient services. While the implementation of HIS faces with several issues that comprising high initial cost, lack of the computer skill, complex task and function, and security and privacy issues.

The most critical issues in implementing the HIS is a security issue, because the type of the data that stores and process in the HIS related to the patient healthcare data and this type of the data are so sensitive and valuable. Therefore, the security of data in HIS is very important (Ismail et al., 2013).

Table 1 - Healthcare Innovation	
No.	Innovation
1	Information Systems (IS)
2	Information and Communication Technology (ICT)
3	Customer-based Inter organizational Systems (CIOS)
4	Electronic Data Interchange (EDI)
5	Cloud Computing
6	Health Level Seven International (HL7)
7	Customer Relationship Management (CRM)
8	Healthcare Information Systems (HIS)
9	E-signature
10	Inter organizational System
11	Electronic Health Record (EHR)
12	Electronic Medical Record (EMR)
13	E-Business
14	Picture Archiving and Communication System (PACS)
15	Mobile Nursing
16	Radio-Frequency Identification (RFID)
17	E-learning

Note: Source: Ahmadi et al., 2015

Methodology

In this research, we applied literature search process approach that proposed by Von Brocke et al. (2009). This research process includes four phases involves journal search,

database search, keyword search, and backward and foreword search, furthermore, in continue evaluate the sources (Figure 2) (Von Brocke et al., 2009).

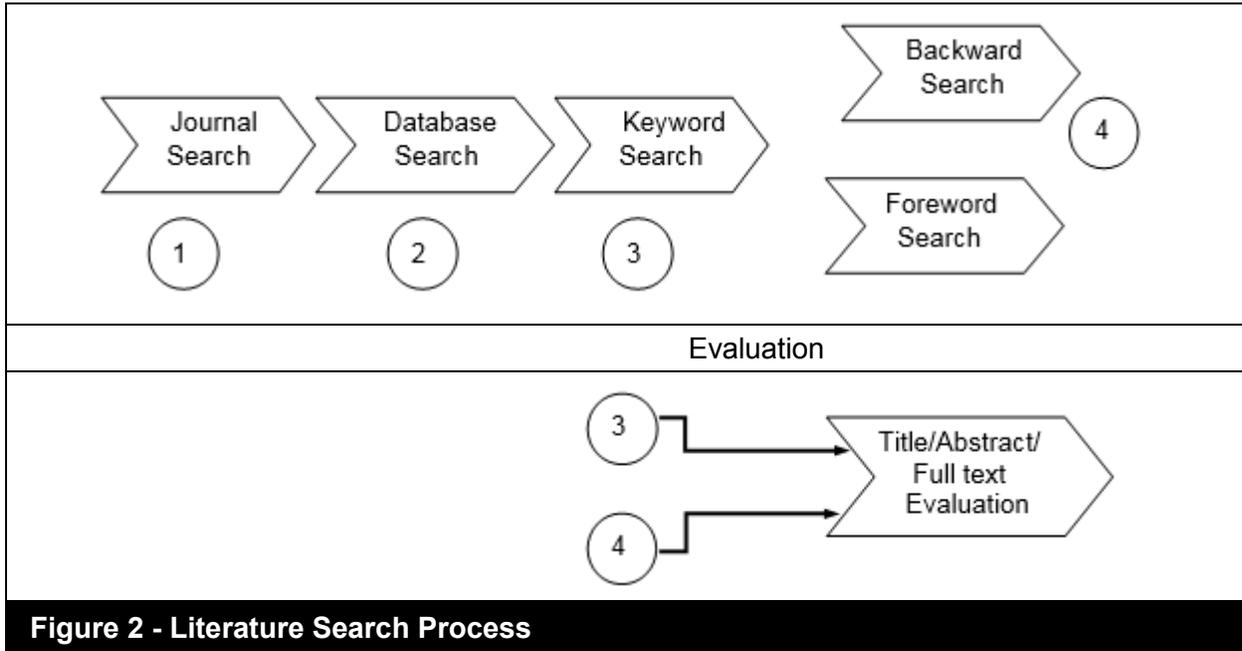


Figure 2 - Literature Search Process

Note: Source: Von Brocke et al., 2009.

First, we identify right journals and databases for searching suitable articles. By searching several databases, we can access to the various journals. We base on AIS World MIS Journal Ranking for IS and Management literature to select conferences and journals. We identified the journals and databases based on keywords search, and then select suitable keywords that related to the research content. In this research, we have selected “hospital information systems”, “HIS”, “HIS issues”, “data security issues”, and “security issues” as keywords, and later used these keywords, and combination of them for searching in several databases and journals to identify the right articles. We found the conference proceeding and journal papers through searching in the EBSCOhost, IEEE Explorer, Emerald, Science Direct, AISel, Springer, ACM Digital Library, and

ProQuest database. Next phase is a backward, foreword search that backward refers to identify and examine the references or works cited in an article of interest, and foreword search process refers to reviewing the extra sources that have cited the articles.

Each phase need evaluation such as assessing, deciding, recommending, selecting, judging, explaining, discriminating, supporting and conducting. In the other words, the articles are selected and identified using keyword search, and backward and forward search that more relevant to the topic and also evaluated articles content that means to analyses title, abstract, and in some case full texts. Since the keywords of this study have several dimensions, therefore, we found 775 articles from the mentioned database, and only 40 of them related to this study. After collecting

adequate articles that related to the topic, then we analyze the articles by separating, connecting, comparing, selecting and describing them. Finally, we discussing and synthesizing the previous researches to reach to the result. For writing, the results derived from each article then summarized as findings of this study.

Data Security Issues

Data security is a complex field that deals with several issues and problems, and provides several solutions as a security and privacy can threaten in the several ways. Solutions normally lead to obstructions in normal use. A global preserving and security solution has to begin with security guideline, security rules and set of the internal privacy definition. These rules must exactly define where the physical place of data is in each stage of lifecycle and they specify how to treat the sensitive data, where it can appear. At the end, patient education is so essential, they should know how the security protecting work and they know about how to resist about the attacker. Data and information security should protect data and information from first stage that data and information create until the last stage, final disposal of the data and information. During the lifetime, the data and information transfer to the several processing systems and in each processing system the data and information can be threat, therefore in order to protect data and information, each processing stage need to provide protection mechanism (Lhotska et al., 2008).

The main goal of data security in HIS is to achieve patient safety and privacy. Patient safety means provide best opportunity for patient to come with right information at the right time, and patient privacy means protecting the sensitive patient data and information from unauthorized person. The system must protect from attacker and any unauthorized access with implementing strong identification and authentication

mechanism. Therefore, the system must guarantee that every user can only access to the data and information, which is permitting to them (Lhotska et al., 2008). Security in HIS is important area that lead to enhance the patient confidently and also lead to public interest to use HIS, while the security in HIS is not fully consider to achieve these goals and several study are still need in this area (Win et al., 2005).

Many studies investigated on the clinic privacy and data security, they found that security vulnerabilities in HIS and in continue they mentioned, considering to security vulnerabilities can be more effectiveness in the security control of HIS. Telemedicine is one of the HIS that provides medical care for patients with the active device such as mobile. This system is very useful but depends on security of system. Using the cloud computing in the HIS is another solution that solve the existing issues and problems in HIS and cloud computing can bring several benefits for HIS and lead to rapidly progress, while security in cloud computing is a main barrier to adopting in cloud computing for HIS (Hajrahimi et al., 2013).

Many quantitative researches had been conducted in HIS area include technical solution to protect the data and information of the patient in the wireless networks of a medical center (Malin, 2007). Other studies have investigated the impact of HIPAA standards (Ferreria et al., 2006; Terry and Francis, 2007). Many quantitative researches in HIS include economic analysis, patients' privacy concern, public policy, fraud control, risk management, and impact of health information technology on medical errors (Miller et al., 2007; Hajrahimi et al., 2013).

The healthcare sector is also experienced the tectonic shift in enablement of healthcare services via the Internet and mobile technology, for example online consultation, e-clinical, and e-prescription. Health bank is a recently advance in the web technology to manage the patient

information. The health bank is a platform to store and exchange the patient information where the patients could deposit and withdraw information. Google health and Microsoft health Vault are examples of the health banking system. Nevertheless, web-based and mobile-based services confront with security issues (Kalorama Information, 2007).

The research area of security and privacy of HIS related to Internet and mobile application is growing (Pyton et al., 2007; Zheng et al., 2007). For instance, the development of privacy preserving trust negotiation protocol for mobile healthcare system that lead to facilitate trust among use of the devices in compliance with predefined access control and disclosure policies. "Cooperative management" is another methodology for assuring the privacy of several stakeholders' integrity via the web-based applications (Chowdhury and Ray, 2007). The Multi-Agent System (MAS) is another approach that used to develop an agent-based system that can cater for distributed processes and this approach use the agents' characteristics such as autonomous, interactive, extendible and mobile to handle the security processes for users in different environments and devices. Approach is used the different types of encryption algorithms with different security strengths in order to provide different security needs (Sulaiman et al., 2012). MLC (Multi Layer Communication) model is another model that based on five layer of communication and this model provides two types of security mechanisms, which are data and/or channel security for wired and wireless devices, with a range of security strengths provided through the symmetric encryptions (Sulaiman et al., 2011). The future success of HIS is more dependent on the how effectively patients can obtain and manage their information securely. Currently, several technology and method (such as encryption, authentication, and disaster recovery) use to provide security platform (Pyton et al., 2007).

To enhance the effectiveness of HIS require collecting, process, transfer, storage and access to the patient health information that lead to increase the issues and challenges that related to the data security (Liu et al., 2005). Issues that related to the data security can be managerial, organizational, and behavioral. Hence, we need to consider more holistic view of data security, processes, people, and incorporating technology (Da Veiga and Eloff, 2007). Healthcare also is not different. It needs considering the inherently sensitive and private nature of data involved; holistic approach is required toward HIS. It is important that system designer using the security mechanism in designing the HIS at the several levels to reduce the risks associated in HIS (Rajan and Ramaswamy, 2010).

In the healthcare sector, it is usually need to share patient data among different hospitals. In this context, patient data releases could have entailed personally identifying information as well sensitive information that may violate privacy. Several health systems store information in the different specific formats. Therefore, for sharing the data among different hospitals, the diversity types of the data create critical problem, although without interoperability, adopting and implementing the HIS will face with several problems. Thus, security and privacy for establishing the inter-operability HIS in exchanging the patient information remain as one of the issues (Brailer, 2005).

The adoption of HIS offers chances for improving the patient care and more efficient practice management (OIG, 2014). The HIS collect a variety of patient data and information represented in many digital and hand-written types, and they are distributed in many departments and units based on the requirement of care providers and the related staffs. Sometimes the data have to exchange and bound in patients' records. In this case, data are very changeable, and the amount increased all the time and the structure depends on uncontrollable variety of external which mostly human factors. In

the context of HIS, patient's health information needs to protect and access by care providers and health administrators. HIS should allow just authorized user with username, and password can access to the patient data. The concept of security is based on the preservation of someone's right to the measures used in order to ensure that this right is not compromised (Lewis et al., 2005). Furthermore, for preventing to lose the patient data, should give backup from the patient information. Efficiency handling the patient information and keeping the patient information safety are to important issues in the HIS (Ismail et al., 2012). Therefore, security can define as the process or means of ensuring that access to, or usage of, protected data is appropriate (Austin and Darby, 2003).

The protection of data and information represents a growing challenge. A series of Office of Inspector General (OIG) audits revealed that some hospitals lack sufficient security features, potentially exposing patients' electronic protected health information to unauthorized access (OIG, 2014). Meanwhile, vulnerabilities included unsecured wireless access, inadequate encryption, authentication failures, and access control vulnerabilities. According to

Roney (2012), hospitals and health systems like HIS are high risk because of the type of data they work with patient personal information, financial information, social security numbers, names, addresses, birth dates and others. The most common causes of data security issues in hospital and HIS are human error, hackers, lost or stolen paper, lost or stolen tapes or compact discs, privacy policy violation, lost or stolen USB, software error, and lost or stolen mobile (Roney, 2012).

Information and data in HIS has different values and may be subject to different regulations. In this context, knowing the value, sensitivity, and importance of hospital data allows for prioritizing the protection measures (Landolt et al., 2012). Further, there are an increasing number of internal and external systems exchange data with each other over the Internet, and the data are subject to data protection law and have to protect. Since the cryptographic controls could allow the exchange of data and guarantees the integrity and authenticity of the data, a policy on the use of cryptography controls are required. Figure 3 illustrates a framework of data security issues as discussed above.

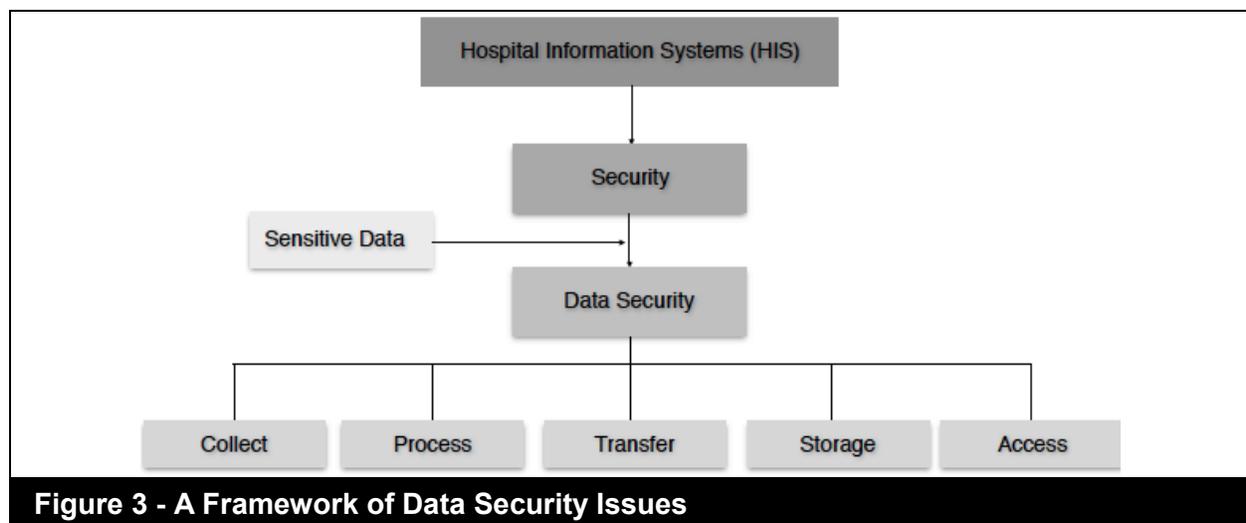


Figure 3 - A Framework of Data Security Issues

According to Wei (2011), the reliability of computer software and hardware system cannot guarantee system security foolproof. However, it could reduce the losses caused by media failure. Lewis et al., (2005) had listed some important points related to the security issues and means that could adopt to overcome them within hospital information systems (HIS), namely:

- A security policy that describes the obligation of the organization (for example, hospitals) to secure their data and assure the appropriateness of their disclosure.
- A map of data assets and its' use across the organization.
- An integrity maintenance plan, that is a plan that describes the maintenance procedures that need to take regularly to ensure the proper function of the security measurements employed in HIS system.
- An intrusion detection plan, that is, a plan showing how and what data or events need to monitor for detecting an ongoing intrusion or abuse of data.
- An intrusion or incident response plan is a plan describing in detail what actual steps need to take for detecting a certain type of intrusion.
- A response plans that compromising patient privacy (for example, logging into records to ascertain their integrity).
- A disaster recovery plan, that is a plan describing in detail how the organizational information system can put back online after an intrusion, or other disaster, forced it to be taken offline or caused corruption of valuable data.
- A communication plan is a plan describing who needs to notify, communicate, and in what channels

in case a breach of security takes place includes both internal and public or patient oriented messaging.

- A clear list is a list notifying who needs to be responsible in the organization for maintaining the different aspects of HIS security.

The developed countries give more emphasis on data and information security of medical organization. Thus, the government should regulate the several rules and norms for medical organization like HIPPA to enhance the service quality to patients and reduce medical resource waste. With present tools and strategies, the defensive strategies of information security arrangement for medical organizations are preceded to prevent the intrusion of hackers, external damages, or internal negligence. And also conform to the regulations of HIPAA that provide the medical organizations with information security concepts to protect the secrets of medical organizations as well as the data and private security of patients (Lui et al., 2012).

Conclusion

Hospitals are part of the important infrastructure of a country, and must protect from data security breaches. The HIS, which encompass services catering to many departments, units, and personnel of hospitals, attempt to satisfy the patient care, and all authorized users such as physicians, nurses, medical technicians, and management personnel. The HIS are not only about computer systems, network, Internet and the applications, but also about the data and information as a whole.

In summary, HIS primarily developed to improve the quality of patient service, to reduce the cost, and to increase the patient's need. HIS need to using the different levels of security for keeping the patient's health information more secure and safe. Ensuring the security of data and information that stored in the HIS is very

crucial; therefore, HIS must provide strong protection for the data and information derived from patient-specific health-related-data. The protection should cover data acquisition, storage, retrieval and linkage activities, and analytic and reporting activities. This paper only covers the technical issues that related to the security issue and not consider to the managerial issue.

In the future, the secure data and information handling in hospitals will increase greatly because of increased information and communication technology usage, and the healthcare information systems will confront with several issues and challenges that need new technology and innovation to solve them. Many researchers attempt to explore in this area and find suitable innovative solutions such as cloud computing to improve the HIS and solve the issues and challenges. These issues will become new area of interest to the IS community that need further studied.

Acknowledgement

We acknowledge to Malaysia Ministry of Education and Research Management Center (RMC), Universiti Teknologi Malaysia (UTM) funded this research project (Project ID: Q.K130000.2540.05H77).

References

Acharyulu G. V. R. K. (2012). "Assessment of Hospital Information System Quality in Multi Specialty Hospitals," *International Journal of Innovation Management and Technology*, 3(4), pp.349-352.

Adler-Milstein, J., and Bates, D. W. (2010). "Paperless Healthcare: Progress and Challenges of an IT-enabled Healthcare System," *Business Horizons*, 53(2), pp.119-130.

Ahmadi, H., Nilashi, M., and Ibrahim, O. (2015). "Organizational Decision to Adopt Hospital Information System: An Empirical Investigation in the Case of Malaysian Public Hospitals," *International Journal of Medical Informatics*, 84(3), pp. 166-188.

Austin, R.D. and Darby, C.A.R. (2003). "The Myth of Secure Computing," *Harvard Business Review*, 81(6), pp.120-126.

Balaraman, P., and Kosalram, K. (2013). "E-hospital Management & Hospital Information Systems – Changing Trends," *International Journal Information Engineering and Electronic Business*, 5(1), pp.50-58.

Biomedical Informatics Ltd. (2006). "Hospital Information Systems," Retrieved from <http://www.biohealthmatics.com/technologies/intsys.aspx> on July 14, 2011.

Brailer, D. J. (2005). "Interoperability: The Key to the Future Health Care System," *HEALTH AFFAIRS-MILLWOOD VA THEN BETHESDA MA-*, 24, W5.

Brocke, J., Simons, A., Niehavas, B., Niehavas, B., Reimer, K., Plattfaut, R., and Anne, C. (2009). "Reconstructing The Giant: On The Importance of Rigour in Documenting the Literature Search Process," *Proceeding of European Conference on Information System (ECIS)*, pp. 161.

Chang, I. C., Hwang, H. G., Hung, M. C., Lin, M. H., and Yen, D. C. (2007). "Factors Affecting the Adoption of Electronic Signature: Executives' Perspective of Hospital Information Department," *Decision Support Systems*, 44(1), pp.350-359.

Chowdhury, A. and Ray, P. (2007). "Privacy Management in Consumer E-health," *Proceedings of 9th International Conference on e-Health Networking, Application and Services*

- (HEALTHCOM), Taipei, Taiwan. pp.29–33.
- Ferreira, A., Cruz-Correia, R., Antunes, L. H. M., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., and Costa-Pereira, A. (2006, June). "How to break access control in a controlled manner," *19th IEEE International Symposium Computer-Based Medical Systems, CBMS*. pp.847-854.
- Garrido, T., Raymond, B., Jamieson, L., Liang, L., and Wiesenthal, A. (2004). "Making the Business Case for Hospital Information Systems," *Journal of Healthcare Finance*. 31(2), pp.21-22.
- Hajrahimi, N., Dehaghani, S. M. H., and Sheikhtaheri, A. (2013). "Health Information security: A Case Study of Tree Selected Medical Centers," *Acta Informatica Medica*. 21(1), pp.42.
- Ismail, A., Jamil, A. T., Fareed, A., Rahman, A., Madihah, J., Bakar, A., Saad, N. M., and Saadi, H. (2012). "The implementation of Hospital Information System (HIS) in tertiary hospitals in Malaysia: a qualitative study," *Malaysian Journal of Public Health Medicine*. 10(2), pp.16-24.
- Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., and Blumenthal, D. (2009). "Use of Electronic Health Records in US Hospitals," *New England Journal of Medicine*, 360(16), pp.1628-1638.
- Kalorama Information (2007) "Wireless Opportunities in Healthcare," Retrieved from www.MarketResearch.com
- Kim, C. Y., Lee, J. S., and Kim, Y. I. (2002). "Early Stage Evolution of a Hospital Information System in a Middle-Income Country: A case study of Korea," *International journal of healthcare technology and management*, 4(6), pp.514-524.
- Landolt, S., Hirschel, J., Schlienger, T., Businger, W., and Zbinden, A. M. (2012). "Assessing and Comparing Information Security in Swiss Hospitals," *Interactive Journal of Medical Research*. 1(2), pp.1-11.
- Lewis, D., Chang, B. L., and Friedman, C. P. (2005). "Consumer health informatics," Springer, New York.
- Lhotska, L., Aubrecht, P., Valls, A., and Gibert, K. (2008, October). "Security recommendations for implementation in distributed healthcare systems," *42nd Annual IEEE International Carnahan Conference Security Technology, ICCST*. pp.76-83.
- Liu, C. H., Chung, Y. F., Chen, T. S., and Wang, S. D. (2012). "The enhancement of security in healthcare information systems," *Journal of medical systems*. 36(3), pp.1673-1688.
- Liu, Y., Clark, J. A., and Stepney, S. (2005). "Devices are People Too Using process patterns to elicit security requirements in novel domains: A Ubiquitous Healthcare Example," *Security in Pervasive Computing, Springer Berlin Heidelberg*. pp.31-45.
- Malin, B. (2007). "A computational model to protect patient data from location-based re-identification," *Artificial intelligence in medicine*. 40(3), pp.223-239.
- Miller, A. R., and Tucker, C. (2007, January). "Privacy, Network Effects and Electronic Medical Record Technology Adoption," *WEIS*.
- Office of Inspector General (OIG). (2014). "Integrity and Security of Health Information Systems and Data," Retrieved from <https://oig.hhs.gov/reports-and-publications/top-challenges/2012/issue09.asp> on June 27, 2014.
- Pan, Z. X., and Pokharel, S. (2007). "Logistics in Hospitals: A Case Study

- of Some Singapore Hospitals,” *Leadership in Health Services*. 20(3), pp.195-207.
- Paré, G., and Elam, J. J. (1999). “Physicians Acceptance of Clinical Information Systems: An Empirical Look at Attitudes, Expectations and Skills,” *International journal of Healthcare Technology and Management*. 1(1), pp.46-61.
- Peyton, L., Hu, J., Doshi, C. and Seguin, P. (2007). “Addressing Privacy in a Federated Identity Management Network for E-health,” *Proceedings of the 8th World Congress on the Management of e-Business, Toronto, Canada*. pp.12–12.
- Rajan, S., and Ramaswamy, S. (2010). “On The Need for a Holistic Approach to Information Quality in Healthcare and Medicine,” *Proceedings of the 48th Annual Southeast Regional Conference. ACM*.
- Ratnam, K. A., and Dominic, P. D. D. (2012). “Cloud Services-Enhancing the Malaysian Healthcare Sector,” *International Conference on Computer & Information Science (ICIS)*. pp. 604-608.
- Roney, K., (2012). “Handle Hospital Data Breaches with Care: 5 Issues to Consider,” Retrieved from <http://www.beckershospitalreview.com/healthcare-information-technology/handle-hospital-data-breaches-with-care-5-issues-to-consider.html> on 28 June 2104.
- Roussel, L., Swansburg, R. C., and Swansburg, R. J. (2006). “Management and leadership for nurse administrators,” *Jones & Bartlett Learning*.
- Sulaiman, H. (2011). “Healthcare Information Systems Assimilation: The Malaysian Experience,” *Doctoral dissertation, RMIT University*.
- Sulaiman, R., Sharma, D., Ma, W., and Tran, D. (2012). “Enhancing Security in E-Health Communications using Multi-Agent System,” *Journal of Computer Science*. 8(5), pp. 637.
- Sulaiman, R., Sharma, D., Ma, W., and Tran, D. (2011). “A new security model using multilayer approach for E-health services,” *Journal of Computer Science*. 7(11), pp. 1691.
- Terry, N. P., and Francis, L. P. (2007). “Ensuring the privacy and confidentiality of electronic health records,” *U. Ill. L. Rev.* pp.681.
- Veiga, A. D., and Eloff, J. H. (2007). “An Information Security Governance Framework,” *Information Systems Management*, 24(4), pp.361-372.
- Wei, X. (2011). “Hospital Information System Management and Security Maintenance,” *Computing and Intelligent Systems Communications in Computer and Information Science*, pp. 418-421.
- Win, K. T. (2005). “A review of security of electronic health records,” *Health Information Management*. 34(1), pp.13-18.
- Yusof, M. M., Papazafeiropoulou, A., Paul, R. J., and Stergioulas, L. K. (2008). “Investigating Evaluation Frameworks for Health Information Systems,” *International Journal of Medical Informatics*, 77(6), pp. 377-385.
- Zheng, Y., Chen, Y. and Hung, P.C.K. (2007). “Privacy Access Control Model with Location Constraints for XML Services,” *Proceedings of the 23rd International Conference on Data Engineering Workshop, Istanbul, Turkey*. pp.371–378.

About the Authors

Maslin Masrom is an Associate Professor, Razak School of Engineering and Advanced Technology (UTM Razak School), Universiti Teknologi Malaysia Kuala Lumpur. She was the Head of Postgraduate Studies from 2010 until 2012, and currently she is the Head of Science, Management and Design at UTM Razak School. She teaches Information Technology Strategy, Management Information Systems, Marketing and E-Business, Quantitative Analysis, and Research Methodology. She has published many technical papers in books, journals and conferences. Her current research area include Information

Technology / Information Systems Management, Information Security Management, Ethics in ICT, Operations Research, and Knowledge Management. Besides teaching, she is actively involved in research activities funded by the university as well as ministries or agencies.

Ailar Rahimly is currently a PhD Student in Universiti Teknologi Malaysia (UTM). She holds a B.Sc in Computer Software engineering and an M.Sc in MBA-IT management. Her main research interests include technology adoption, cloud computing, security in cloud computing and healthcare information systems.